

# **Email Training**

June 17, 2009

Email is probably the most challenging type of electronic record to try to manage. Businesses, governments, and entire nations have been trying for at least a decade to find an easy solution. There isn't one. Yes, there are technologies that can help. But technology is only one factor. Human beings have to live with the solution, and often that's a very hard sell.

Why is it important to manage email?

It's easy to downplay the risks of not managing email, especially if your office has never been sued and attorneys aren't trying to hunt for relevant information in your in-box or out-box. Also, you may not realize the significance of the storage issues that your IT people face as they try to support your email needs. Sometimes your IT department may set limits on the size of your account, and insist that you clean it out periodically, or else they will do it for you on a set time schedule (even if the email is important). Another risk that's kind of hidden is your agency's ability to document its own decisions, if documentation is only contained in email.

For instance, part of my job is to order new computers and software for our office. I can't tell you how many times someone has asked me for information related to a purchase that happened years before, and the only documentation I have is contained in an email. It's a good thing I keep those emails, because otherwise we could not have proved that we paid for software licensing, and then we would have been stuck with a very large bill. The email that proved the point was 8 years old, well beyond the normal 3-year retention that happens with other purchasing documentation. In my case, someone else was supposed to keep the purchasing documentation, and didn't, so the email was the only evidence.

How long should you keep email?

From the survey that Rosemary sent out a couple of weeks ago to local government agencies, many of you have questions about how long email should be kept. The answer is: that depends. The temptation for many is to delete email when you feel like it, or to put it more formally, "Retain in office until administrative need ends and then destroy." That means some people will keep it forever even if they never look at it again, and others will delete the email immediately, even if they need to act on the information later. Another temptation is to view all email as a single entity just because it comes to you through a single portal, so "email" becomes the title of the series, instead of just one piece of a customer case file.

In our general retention schedules, we do categorize correspondence by its content: transitory correspondence can be destroyed anytime, and policy and program correspondence should be kept permanently. The description for transitory correspondence is:

This is business-related correspondence that is routine or transitory in nature and does not offer unique information about agency functions or programs. These records include acknowledgment files and most day-to-day office and housekeeping correspondence. These records may originate on paper, electronic mail, or other media. This correspondence is filed separately from program and project case files.

The description for policy and program correspondence is:

Business-related correspondence which provide unique information about agency functions, policies, procedures, or programs. These records document material discussions and decisions made regarding all agency interests, and may originate on paper, electronic mail, or other media. This correspondence is filed separately from program case files, and project files.

Just because we acknowledge these two general buckets of information should not preclude you from creating your own categories for certain types of email. You can create a retention schedule that says “Email relating to software purchases should be retained until the software is replaced and then destroy.” Or you could have a policy that certain email is to be considered part of the agency’s normal case files, in which case you don’t file the email as “correspondence.” Instead, the retention of the case file takes precedence over the retention for email correspondence.

Sometimes the important part of the email is the attachment, and that attachment may have a retention that is entirely different from the email it came with. Be careful to decide which copy of something is the record copy in your office, because that is the copy that will be kept the longest. For email, the out-going email is generally the record copy, so the person who sent the email should keep it for the longest period of time. If an email came to you from outside government, then the incoming copy is the record copy. For email threads where an entire conversation is contained within every email, the last response is the record copy.

Policy and program correspondence—the really permanent kind—should be relatively rare in your office. It would include information not contained anywhere else and truly document unique decisions and policy discussions. These emails would likely be written by department directors or elected officials rather than line staff, and as such a series title of “director’s correspondence” would be appropriate.

Not every email is going to be a business record. If your director emails his mother to tell her happy birthday, that’s not a record, and you don’t need to keep it. If you do keep it, note that the email is still discoverable for litigation purposes. This category of email falls under acceptable use rules rather than email retention schedules. If your agency is part of state government, there is an administrative rule for acceptable use of the state’s computer systems. Local governments often adopt similar policies. For instance, the state’s acceptable use rule allows for these kinds of conditions:

- An employee may engage in incidental and occasional personal use of IT resources provided that such use does not:
  - Disrupt or distract the conduct of state business due to volume, timing, or frequency;
  - Involve solicitation;
  - Involve for-profit personal business activity;
  - Involve actions, which are intended to harm or otherwise disadvantage the state; or
  - Involve illegal and/or activities prohibited by this rule.

A records management policy, on the other hand, is different from an acceptable use policy. It focuses on the risks to the organization when records are not managed appropriately.

The Archives has written a new set of guidelines for email, which is a type of records management policy. You should have a copy in your packet. It's also on our website. These guidelines lay out why email is such a problem, and what you can do to limit your risks. To fully implement these guidelines, some kind of recordkeeping software is required. Basically, the guidelines call for email to be transferred out of their originating email system, be that GroupWise, Outlook, or even g-mail, and into a recordkeeping system that will tag each email with a retention schedule. Email copies still in the email system are destroyed promptly such as every 30 days, including the email backup. The recordkeeping system backup would reflect the retention schedules of the items it is managing. Backups would be used for disaster recovery, not e-discovery. The recordkeeping system would manage access to the emails, be searchable, and be able to prevent email from being deleted if the user needed to put a hold on it for litigation. Email of permanent value could also be transferred from this system to Archives on a regular basis, such as every 5 years.

If you turn with me to page 4 in the email guidelines, under the heading Policy Components, it says:

The goal of an e-mail management system is to manage e-mail from creation or receipt to destruction or permanent preservation. The policy that governs that program must address—but not necessarily be limited to—the following points:

**Essential Elements of the E-mail Management System**

Require, via policy, administrative rule, or statute, that each State agency uses an approved electronic records management system or develop a policy of their own that is in compliance with the baseline standards of said system. A management system includes the hardware, software, and storage medium used to manage e-mail, and the policy describes how the system is used and the records it contains. To ensure that all essential e-mails are accessible within the management system, the policy must

require that all State business is conducted on computers and devices that are connected to an authorized management system.

So these guidelines outline the baseline standards needed in a recordkeeping system for managing email. With these standards in place, agencies are then encouraged to create their own policies to ensure legal compliance, with enough flexibility built in to fit their unique requirements.

These guidelines do mention some acceptable use elements, particularly when an employee receives an email that could potentially explode into a lawsuit. When this is the case, the employee is required to take proactive steps to make sure the email is saved. If that is not done, your agency could be exposed to legal risks. This kind of responsibility on the part of every end user requires a fair bit of training. As records officers, your ability to communicate this need to your fellow employees is critical. If you turn to page 6 in the email guidelines, let's look at what it says about e-discovery:

Both the federal and Utah Rules of Civil Procedure expressly provide for the discovery in litigation of all discoverable electronically created or stored information, including e-mails, in their electronic format. Electronically stored or created information can be regularly destroyed without penalty under these rules if the destruction was pursuant to a reasonable electronic records management system that is consistently implemented and followed within the agency.

This "safe harbor" is suspended, however, when a "litigation hold" has been, or should have been, put in place. A litigation hold is an internal directive to preserve all relevant information, including electronically created or stored information, which is in the possession, custody, or control of the agency.

The obligation to implement a litigation hold is triggered as soon as the agency knows, or should have known, that litigation regarding the matter at issue was reasonably foreseeable. Once a litigation hold is implemented, all deletion or destruction protocols with regard to electronically created or stored information that may relate to the matter at issue must be immediately suspended. Those records must thereafter be preserved in their electronic format until any litigation is concluded or the litigation hold is appropriately lifted.

There are penalties for not complying with litigation rules. So you can see that it is very advantageous for an agency to implement a real recordkeeping system for email.

At the moment, with budget issues being what they are, not many agencies can afford to purchase and maintain a full-blown recordkeeping system. So what can you do in the meantime?

First, realize that without the actual recordkeeping system, you will face all the risks from litigation that you currently do. What may improve is your ability to find a specific email a little easier. While you may be able to delete email manually according to retention schedules, realize that the backup copies will still exist. If you choose to print and file email, you will lose the metadata that comes with that email, such as when the email was opened by the recipient. Sometimes those details are important, and printed copies may not meet the requirements of a legal challenge, although they would help the agency document its own decision-making.

To manage these records manually, in your email client, create folders that will help you organize your email by subject, record series, or retention schedule. When you send or receive an email related to that category, drag the item into the folder. Then periodically go through the folders, sort the records chronologically, and delete the ones whose retention has been met.

If you would like to explore the purchase of an actual recordkeeping system, there are many on the market. These can be integrated with your email client. Some offer the ability to categorize records by rules, meaning that they don't interrupt the end user with a bunch of questions each time an email is sent, but manage to assign it to a retention schedule just the same. Nice as that sounds, I don't believe there is a truly elegant solution for email yet. The best option is probably some kind of mix between user-tagged and system-tagged email. An example of a retention rule is to make any email you send to your mother's email address a non-record. Any email sent to a listserv is transitory. To be able to categorize emails more easily, the guidelines suggest making the subject line of your outgoing email meaningful. In other words, don't just title your email "hello" and then in the message body proceed to talk about how you intend to reinvent government in your organization.

At the state, we are beginning to investigate a product called Nexic Discovery, which has the ability to remove email from GroupWise's proprietary system and place it into a SQL database that is very searchable. The client behaves in a very similar way to the GroupWise client, so user training is minimal. You can also forward and restore messages from the archive back into GroupWise. It only stores one copy of an email, even if that email was sent to multiple people, and it keeps track of email threads. The product does not provide recordkeeping services such as retention scheduling or litigation holds. It does have the advantage of putting the email in a non-proprietary format, which can be exported and taken with you if you leave state employment and want copies.

If you do a Google search on the term "email archiving" you will come up with several products. Among them are Autonomy Zantaz and ZL Technologies. I haven't used either one, but their product literature suggests that their email archiving solution incorporates retention rules. These may work with email clients such as Outlook Exchange, or Lotus Notes, but perhaps not GroupWise.

Other popular recordkeeping systems include Microsoft Sharepoint and EMC's Documentum. These products can be used with other electronic records, too, not just

email. All of these systems have strengths and weaknesses. Some are good for enterprise collaboration, others have greater strengths in document management or searchability. Still others just provide a way to export email from a system and park it somewhere.

Of course, technology is only part of the problem when it comes to managing email. Even if you find a perfect system, you still need to convince people in your office to use it and not resent it. Conventional wisdom from those who have tried implementing a recordkeeping system say that for it to work, you must have management buy-in, and then when you deploy it, use a pilot project first. Get feedback. Find out what works and what doesn't, then work with your IT staff and your vendor to solve problems. Some solutions may have lots of wonderful features, but also may be really complicated to use. Perhaps you don't need to install all modules, or maybe you just need to turn off some system rules that get in your way. People must incorporate solutions into their daily workflow and that requires change, forethought, planning, and communication. As you prepare to roll out the system to more user groups, understand that some people will always resist and try to get around the system.

User training is necessary: not just the "how" but also the "why." Yes, it takes an extra step to assign that email to a retention schedule, but there is also some greater societal benefit. The less money you are required to spend on email storage, the fewer budget cuts you may have to deal with in other areas. There is no good reason why you should have to spend money on something you don't need, and storing months or years worth of gigabytes for important messages such as "please contribute to the charitable fund drive" is ridiculous. Think of it like when you first learned how to recycle your trash. At first it took a little time to get used to putting your newspapers and plastic bottles in one trash can, and your chicken bones in another, but now it's second nature.

You may not believe me about the storage costs of email, but just consider:

- 11 billion emails a day are sent in the US alone, not including spam
- 75% of civil discovery is for email
- 300+GB email per month are needed for 1,000-user company on average, which for the size of state government's 23,000 employees comes to about 7 TB.
- Add to the storage costs all the costs to manage the email and back it up, and then restore if necessary
- It costs about \$2 per message to produce a record for discovery, or \$2,000 - \$18,000+ per GB
- Costs for not producing a record for discovery are considerably higher

I asked one of the state's email administrators to comment on these statistics. Here is what she said: "Some of our post offices are small because the department does an automatic expire and reduce where they delete ALL messages older than 90 or 180 days. But the post offices that don't run the expire/reduce are much bigger. For example, [one] hosts 650 users and is nearly 500 GB now. [Another] hosts 532 users and stores well over 300 GB. We made a spread sheet last September [that lists storage used per post office]. All of the post offices are at least 10% bigger now. Email storage is a huge issue.

Not just in the cost of the storage, but for the maintenance of the post office. When we run our weekend maintenance routine on [one post office], it runs for over 70 hours. That doesn't address how long backups and restores take. It's just too much data.”

This comment tells me that some of you may be destroying records in contravention of established retention schedules. Remember, retention schedules follow the content of a record, not the system it came from (meaning email). And now the GRAMA law has stipulations with criminal penalties for destroying records that should be kept. So this problem deserves some attention.

For those of you who have tried implementing an email solution, what kinds of problems have you encountered, from either people or the technology?